PENGARUH PENAMBAHAN FUNGSI LINEAR DAN FUNGSI NONLINEAR TERHADAP KEKUATAN S-BOX S1 CLEFIA

Amas

Badan Siber dan Sandi Negara
Jl. Harsono RM No. 70, Jakarta Selatan
amas@bssn.go.id

Abstract - Sbox is a function that widely used in designing symmetric encryption algorithms. This function is nonlinear, designed with some criteria, and one of the important functions that determine the strength of the asymmetric encryption algorithm. Choosing a good s-box is one of the important things in designing of symmetric encryption algorithms because it must ensure its resistance to the common cryptanalysis attack, such as *Linear* and *Differential cryptanalysis*. For these criteria, the s-box must have a good result on *Linear Approximation Table (LAT)*, *XOR Table,* and *Nonlinearity* testing. In this study, the author will generate a new s-box from S1 Clefia's s-box by applying a linear function, nonlinear function, and combination of both to the S1 Clefia. We use S1 Clefia because it has good criteria based on the *Linear Approximation Table (LAT), XOR Table,* and *Nonlinearity* testing. A total of 5 (five) new s-boxes generated by this method and then their strength will be evaluated based on the same testing method. Besides, *Strict Avalanche Criterion (SAC)* and *Bit Independence Criterion (BIC)* tests are applied to ensure that the sbox has good diffusion so that it's difficult to analyze.
Keywords - S-Box, S1 Clefia, *Linear* and *Differential Cryptanalysis, Linear Approximation Table (LAT), XOR Table, Nonlinearity, Strict Avalanche Criterion (SAC)* and *Bit Independence Criterion (BIC).*

Abstrak **–** Sbox merupakan salah satu fungsi yang banyak digunakan dalam mendesain algoritma enkripsi simetrik. Fungsi ini bersifat nonlinear, didesain dengan kriteria khusus dan menjadi salah satu tolak ukur kekuatan suatu algoritma enkripsi simetrik. Pemilihan s-box menjadi salah satu hal penting dalam desain algoritma enkripsi simetrik, karena harus memastikan ketahanannya terhadap standar serangan yang ada saat ini, diantaranya *Linear* dan *Differential cryptanalysis*. Untuk memiliki kriteria tersebut, maka s-box harus memenuhi kriteria yang baik berdasarkan pengujian *Linear Approximation Table (LAT), XOR Table* dan *Nonlinearity*. Pada penelitian ini, penulis membangkitkan s-box baru dari s-box S1 Clefia dengan cara menerapkan suatu fungsi linear, fungsi nonlinear dan kombinasi keduanya terhadap s-box S1 Clefia. Penulis menggunakan s-box S1 Clefia karena memiliki kriteria yang baik berdasarkan pengujian *Linear Approximation Table (LAT), XOR Table* dan *Nonlinearity*. Sebanyak 5 (lima) buah s-box baru dibangkitkan dari penerapan fungsi tersebut, kemudian s-box baru tersebut dievaluasi kekuatannya dengan metode pengujian yang sama. Selain itu dilakukan pula pengujian *Strict Avalanche Criterion (SAC)* dan *Bit Independence Criterion (BIC)* untuk meyakinkan bahwa sbox yang dihasilkan memiliki tingkat difusi yang baik sehingga sulit untuk dianalisis.
Kata Kunci – S-Box, S1 Clefia, *Linear* dan *Differential Cryptanalysis, Linear Approximation Table (LAT), XOR Table, Nonlinearity Strict Avalanche Criterion (SAC)* dan *Bit Independence Criterion (BIC).*

I. PENDAHULUAN

Sebagai salah satu metode yang digunakan dalam rangka melindungi keamanan informasi, algoritma kriptografi menjadi salah satu cabang ilmu pengetahuan dan teknologi yang berkembang pesat saat ini. Hal ini dikarenakan keamanan informasi merupakan kebutuhan utama seiring dengan perkembangan TIK. TIK memiliki dampak negatif berupa maraknya kejahatan siber yang muncul dari adanya kerentanan sistem TIK. Dengan terpenuhinya kebutuhan keamanan informasi akan meningkatkan kepercayaan masyarakat terhadap TIK dan tentunya melindungi masyarakat dari dampak buruk perkembangan TIK.

Perkembangan algoritma kriptografi saat ini tidak terlepas dari perkembangan fungsi matematika dan komputasi. Algoritma kriptografi yang ada umumnya dibangun dari fungsi-fungsi matematika yang telah terbukti secara ilmiah memiliki kriteria yang dibutuhkan. Fungsi-fungsi matematika tersebut tentunya melalui proses pengujian dan pembuktian kekuatan berdasarkan metode yang dapat dipertanggung jawabkan. Selain itu fungsi yang digunakan harus mudah untuk diimpelemantasikan.

Salah satu algoritma yang sering digunakan saat ini yaitu algoritma enkripsi simetrik. Algoritma ini menggunakan kunci yang sama untuk mengenkripsi maupun mendekripsi pesan, sehingga hanya pihak yang memiliki kunci yang dapat mengetahui isi dari pesan. Algoritma ini banyak digunakan pada sesi komunikasi yang membutuhkan kecepatan dan pada enkripsi data dalam jumlah yang relatif besar.

Algoritma enkripsi simetrik memiliki komponen utama berupa fungsi yang dapat mempengaruhi kekuatan dari algoritma. Salah satu fungsi yang sering digunakan dalam mendesain algoritma enkripsi simetrik yaitu s-box. Fungsi ini biasanya bersifat nonlinear dan menjadi salah satu tolak ukur kekuatan dari algoritma. karena berukuran relatif kecil sehingga lebih mudah untuk dianalisa kekuatannya.

S-box memiliki kriteria yang harus dipenuhi agar efektif dalam mendukung kekuatan algoritma secara keseluruhan. Pembangkitan s-box yang memenuhi kriteria membutuhkan penelitian lebih lanjut. Selain itu, terdapat isu lain yaitu apakah suatu s-box yang baik akan tetap mempertahankan sifatnya saat dikombinasikan atau dioperasikan dengan suatu fungsi.

Berdasarkan hal tersebut, penulis melakukan penelitian yang berjudul Pengaruh Penambahan Fungsi Linear dan Fungsi Nonlinear Terhadap Kekuatan S-Box S1 Clefia. Hasil yang diharapkan dapat memberikan gambaran mengenai pengaruh fungsi-fungsi tersebut terhadap salah satu s-box yang sudah lulus uji (S1 Clefia). Hal ini dapat menjadi gambaran dan pertimbangan dalam membangkitkan s-box baru dari s-box yang sudah ada.

A. Fungsi Linear

Fungsi linear merupakan suatu fungsi boolean f yang memenuhi kondisi:

$$(f \oplus g)(X) = f(X) \oplus g(X)$$

$$(c.f)(X) = c.f(X)$$

untuk setiap x, y pada F_2^ndan c pada F_2. Suatu fungsi linear $f$jika di representasikan dalam bentuk Algabraic Normal Form (ANF) maka akan menjadi:

$$f(x_1, x_2, \dots, x_n) = f(e_1 x_1) \oplus f(e_2 x_2) \oplus \dots \oplus f(e_n x_n)$$

$$f(x_1, x_2, \dots, x_n) = f(e_1) x_1 \oplus f(e_2) x_2 \oplus \dots \oplus f(e_n) x_n$$

$$f(x_1, x_2, \dots, x_n) = a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n$$

dimana $f(e_i) = a_i$untuk a di F_2, $i = 1,2, \dots, n$[1].

B. S-box S1 CLEFIA

CLEFIA merupakan algoritma yang telah ditetapkan sebagai salah satu standar algoritma *lightweight block cipher* berdasarkan ISO/IEC 29192-2, memiliki kriteria khusus untuk penerapan pada *device* dengan sumberdaya terbatas. Algoritma ini berbasis *block cipher* dengan ukuran 128 bit blok dengan variasi kunci 128, 192 dan 256 bit.

CLEFIA memiliki fungsi F sebagai komponen utama dalam struktur algorimanya. Pada fungsi F tersebut terdapat fungsi *nonlinear* S-box 8x8 dan fungsi *linear mixing*. S-box pada algoritma CLEFIA terdiri dari 2 buah S-box S0 dan S1.

S1 Clefia merupakan Sbox 8x8 yang didefinisikan sebagai berikut :

$$y = \begin{cases} g(f(x)^{-1}) \text{ jika } f(x) \neq 0 \\ g(0) \quad\quad\quad \text{jika } f(x) = 0 \end{cases}$$

Fungsi invers dibentuk dalam $GF(2^8)$ yang didefinisikan dalam polynomial $\boldsymbol{z^8 + z^4 + z^3 + z + 1}$. Fungsi f(.) dan g(.) adalah transformasi *affine* pada $GF(2)$ dengan definisi sebagai berikut.

$$f: \begin{cases} \{0,1\}^8 \rightarrow \{0,1\}^8 \\ x_{(8)} \rightarrow y_{(8)} \end{cases}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$g: \begin{cases} \{0,1\}^8 \rightarrow \{0,1\}^8 \\ x_{(8)} \rightarrow y_{(8)} \end{cases}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Nilai x dan y didapatkan dari nilai $x_0|x_1|x_2|x_3|x_4|x_5|x_6|x_7$ dan $y_0|y_1|y_2|y_3|y_4|y_5|y_6|y_7$[6].

C. Linear dan Differential cryptanalysis

Linear dan *Differential cryptanalysis* merupakan jenis standar serangan yang umum digunakan untuk mengetahui kekuatan dari suatu algoritma enkripsi simetrik. Kedua serangan ini tergolong dalam *known plaintext attack*, dimana membutuhkan sejumlah pasangan plainteks untuk menemukan informasi tentang kunci.

Linear cryptanalysis merupakan serangan yang berdasarkan pada aproksimasi hubungan *linear* yang efektif antara plainteks, cipherteks dan kunci[5]. *Differential cryptanalysis* merupakan serangan yang menggunakan propagasi *differ* input dan *differ* output, yaitu karakteristik tentang XOR dari 2 input dengan XOR dari 2 output yang berkorespondensi[3].

Untuk melihat ketahanan algoritma enkripsi simetrik, maka komponen nonlinear yang menjadi inti seperti sbox pada algoritma harus dilakukan pengujian, diantara nya yaitu *Linear Approximation Table (LAT), XOR Table* dan *Nonlinearity*.

D. Linear Approximation Table (LAT)

Merupakan alat uji yang berbentuk tabel distribusi yang didefinisikan sebagai jumlah semua variasi dari input *x* yang menyebabkan nilai operasi *dot product* antara input dengan α sama dengan nilai operasi *dot product* antara output dengan *β*.

Misal sebuah fungsi nonlinear $f = (X) = Y, f: \{0,1\}^n \rightarrow \{0,1\}^n$ dapat membentuk sebuah fungsi linear yang dinyatakan sebagai:

$$X_1 \oplus X_2 \oplus \dots \oplus X_n \oplus Y_1 \oplus Y_2 \oplus \dots \oplus Y_n = 0$$

Semua kemungkinan fungsi linear yang mungkin terjadi pada fungsi non-linear dapat dihitung dengan menggeneralisasi fungsi linear diatas menjadi:

$$\alpha_1.X_1 \oplus \alpha_2.X_2 \oplus \dots \oplus \alpha_n.X_n \oplus \beta_1.Y_1 \oplus \beta_2.Y_2 \oplus \dots \oplus \beta_n.Y_n = 0$$

Disederhanakan menjadi

$$\underset{i=1}{\overset{n}{XOR}}(X_i.\alpha_i) = \underset{i=1}{\overset{n}{XOR}}(Y_i.\beta_i)$$

$$LAT(\alpha,\beta) = \#\{X \mid X \in Z_2^n, \underset{i=1}{\overset{n}{XOR}}(X_i.\alpha_i) = \underset{i=1}{\overset{n}{XOR}}(Y_i,\beta_i)\}$$

Tabel LAT yang digunakan merupakan hasil LAT dikurangi 2^{n-1} sehingga didapatkan :

$$LAT'(\alpha,\beta) = |LAT(\alpha,\beta) - 2^{n-1}|$$ [4]

E. XOR Table

Merupakan alat uji yang berbentuk tabel distribusi yang merangkum seluruh kemungkinan kemunculan pasangan $P1 \oplus P2 = C1 \oplus C2$

Jika diasumsikan penyerang dapat memilih *plaintext* dan *ciphertext* (*Choosen Plaintext Attack*) maka penyerang dapat menggali karakteristik dari persamaan $P1 \oplus P2 = C1 \oplus C2$. Dengan merangkum seluruh kemungkinan kemunculan pasangan $P1 \oplus P2$ dan $C1 \oplus C2$. Penyerang dapat memilih pasangan *plaintext* yang memiliki *difference* ΔP yang sedemikian hingga memiliki peluang yang besar untuk menghasilkan *difference* output ΔC untuk kemudian dicari bit-bit kunci yang terafiliasi.

XOR table dapat dikonstruksikan sebagai berikut :

$$XOR(\Delta P, \Delta C) = \#\{P \mid f(P) \oplus f(p \oplus \Delta P) = \Delta C\}$$ [4]

F. Nonlinearity

Nonlinearity dari suatu fungsi didefinisikan sebagai minimum jarak hamming (*hamming distance*) antara fungsi tersebut dan setiap fungsi linear atau fungsi affine. *Nonlinearity* dari suatu fungsi Boolean adalah

$$NL(f) = \min_{a \in \mathbb{F}_2^n} d_H(f, \ell_a \oplus b)$$

dengan $\ell_a \oplus b$ menyatakan fungsi boolean affine yang didefinisikan oleh vektor biner a. $\ell_a = a \cdot x$ ($\cdot$ merupakan perkalian titik). d_H menyatakan jarak hamming.

Jarak hamming d_H dapat diekspresikan menggunakan *Walsh-Spectrum* dari f, sedemikian sehingga nilai $NL(f)$ dapat dihitung sebagai

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m} |\mathcal{W}_{F \cdot b}(a)|$$

dengan $\mathcal{W}_{F \cdot b}(a) = \mathcal{W}_F(a,b)$ merupakan transformasi walsh dari f.

Nonlinearity berkaitan secara langsung dengan LAT (*Linear Approximation table*). Jika $\gamma = \max_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m} |LAT(a,b) - 2^{n-1}|$, maka nonlinearity dari *F* dapat dihitung melalui persamaan berikut

$$NL(F) = 2^{n-1} - \gamma$$ [2]

G. Strict Avalanche Criterion

Sebuah fungsi $f : Z_2^n \rightarrow Z_2^m$ dikatakan memenuhi *Strict Avalanche Criterion* (SAC), jika seluruh *i*, di mana ($1 \leq i \leq n$) memenuhi persamaan :

$$\sum_{x \, E \, z n_2} ((\,) f\, x \oplus f\, x(\, + c_i^{(\,)n})) = (2^{n-1}, 2^{n-1}, \dots, 2^{n-1})$$

Dalam hal ini jika perubahan satu bit input, maka setiap bit *output* akan berubah dengan probabilitas setengah. Berdasarkan persamaan tersebut, maka dapat diperoleh persamaan baru, yaitu parameter SAC (K_{SAC}), persamaan tersebut, adalah :

$$K_{SAC}(i, j) = 1/2^n \; wt\,(f(x) \oplus f(x \oplus c^n{}_i)) = ½$$

di mana $1 \leq j \leq m$.

Dengan demikian $K_{SAC}(i, j)$ dapat bernilai antara "0" nol "1" atau satu, dan sebuah *sbox-0* dikatakan memenuhi kriteria SAC jika nilai K_{SAC} (i, j) untuk semua *i* dan *j* bernilai tepat setengah[7].

H. Bit Independence Criterion

Bit Independence Criterion (BIC) menyatakan bahwa setiap bit pada *avalanche vector* harus saling lepas (bersifat *independence*). Secara matematika BIC dapat didefinisikan sebagai sebuah fungsi $f: \{0,1\}^n \rightarrow \{0,1\}^n$ untuk semua $i, j, k, \varepsilon \{1,2,\cdots,n\}$ dengan $j \neq k$, jika bit input ke i diubah, maka akan menyebabkan perubahan yang saling bebas (*independently*) pada output bit ke j dan k berdasarkan pada nilai koefisien korelasinya. Persamaan koofisien korelasi yang digunakan pada pengujian BIC adalah :

$$BIC^{ei}(A_j, A_k) = |corr(A_j^{ei}, A_k^{ei})|$$

Secara keseluruhan, BIC sebuah fungsi boolean $f: \{0,1\}^n \rightarrow \{0,1\}^n$ dapat didefinisikan sebagai:

$$BIC(f) = max(BIC^{ei}(A_j, A_k)) \text{ untuk } 1 \leqslant i \leqslant n$$

dan $1 \leqslant j, k \leqslant n$ dan $j \neq k$[7].

II. METODE PENELITIAN

Pada paper ini, penulis melakukan metode penelitian sebagai berikut :

1. Pembangkitan s-box baru
   Pembangkitan s-box baru dengan menggunakan penambahan fungsi atau operasi baik linear maupun nonlinear terhadap sbox S1 CLEFIA. Fungsi linear yang digunakan pada penelitian ini

dibatasi dengan menggunakan operasi-operasi sebagai berikut :

a. Rotasi bit, yaitu menggunakan rotasi bit ke kanan sebanyak 5 (x >>> 5)
b. Perkalian input *x* dengan suatu nilai konstanta pada GF(2^8) dengan polinomial $f(x) = x^8 + x^4 + x^3 + x + 1$. Polinomial ini merupakan polinomial *irreducible* yang digunakan pada algoritma enkripsi AES
   Konstanta yang digunakan pada penelitian ini yaitu 0x4, 0x6 dan 0x10 dinotasikan Mul4AES(), Mul6AES() dan Mul10AES().

Pada penelitian ini pembangkitan sbox dengan fungsi linear menggunakan kombinasi operasi a dan b untuk menghasilkan 3 (tiga) buah s-box sesuai pseudocode pada Gambar 1

Pembangkitan sbox dengan penambahan fungsi nonlinear, menggunakan fungsi nonlinear sbox AES. Pada penelitian ini penambahan fungsi nonlinear serta kombinasi fungsi nonlinear dan linear dibatasi menggunakan operasi sebagai berikut :

a. Sbox AES dioperasikan terhadap input sbox S1 CLEFIA.
b. Kombinasi fungsi nonlinear dan fungsi linear dengan ketentuan operasi berikut :
   Sbox[] : S1-Clefia(Mul6AES(sboxAES(i))) >>> 5

Berdasarkan hal tersebut, pembangkitan s-box pada penelitian ini menghasilkan 5 (lima) buah s-box baru dengan proses pembangkitan sesuai dengan pseudocode berikut :

```
Sbox-e[256]
for i = 0 to 255
   do
     x[i] = Mul4AES(i);
     y[i] = S1_Clefia[x[i]]
            >>> 5;
Return y[i]
```

```
Sbox-e[256]
for i = 0 to 255
   do
     x[i] = Mul6AES(i);
     y[i] = S1_Clefia[x[i]]
            >>> 5;
Return y[i]
```

```
Sbox-e[256]
for i = 0 to 255
   do
     x[i] = Mul10AES(i);
     y[i] = S1_Clefia[x[i]]
            >>> 5;
Return y[i]
```

```
Sbox-d[256]
for i = 0 to 255
   do
     x[i] = sboxAES[i];
     y[i] = S1_Clefia[x[i]];
Return y[i]
```

```
Sbox-e[256]
for i = 0 to 255
   do
     x[i] = sboxAES[x[i];
     xx[i]= Mul6AES(i);
     y[i] = S1_Clefia[xx[i]]
            >>> 5;
Return y[i]
```

Gambar 1. Pseudocode pembangkitan s-box

2. Pengujian s-box baru

Pengujian ini dilakukan terhadap 5 (lima) buah sbox yang dihasilkan menggunakan sampel masing-masing sbox sebanyak populasi keseluruhan input s-box yaitu 2^8. Pengujian yang dilakukan sebagai berikut :

a. *Linear Approximation Table (LAT)*
   Pada pengujian ini dihitung Tabel LAT berukuran 256x256 untuk masing-masing Sbox. Penghitungan setiap elemen Tabel LAT dihitung berdasarkan rumus pada Bab II.D. Pada pengujian ini, dicari nilai maksimum *LAT* yang diperoleh.
b. *XOR Table*
   Pada pengujian ini, dihitung Tabel *XOR distribution* berukuran 256x256 untuk masing-masing Sbox yang setiap elemen tabel dihitung berdasarkan rumus pada Bab II.E. Kemudian dicari nilai *differential uniformity* yang merupakan nilai maksimum elemen pada *XOR distribution*.
c. *Nonlinearity*
   Pada pengujian ini dihitung nilai *nonlinearity* masing-masing sbox sesuai dengan persamaan pada Bab II.F.
d. *Strict Avalanche Criterion* (SAC)
   Pada pengujian ini dihitung nilai error maksimal (*Max Error*) SAC berdasarkan rumus pada Bab II.G. Nilai *Error* ini merupakan selisih antara nilai SAC dengan nilai idealnya yaitu ½. Nilai SAC yang baik yaitu ketika *Max Error* yang mendekati nol. Ambang batas nilai *Max Error* ditentukan sebesar 0,1 sehingga dianggap tidak memenuhi jika *Max Error* > 0,1.
e. *Bit Independence Criterion* (BIC)
   Pada pengujian ini dihitung nilai korelasi maksimal berdasarkan rumus pada Bab II.H. semakin kecil nilai korelasi maksimalnya maka semakin baik kriteria BIC nya. Ambang batas nilai korelasi maksimal ditentukan

sebesar 0,2 sehingga nilai BIC dianggap tidak memenuhi jika korelasi maksimal > 0,2.

3. Analisis Hasil Uji
   Analisis hasil pengujian dilakukan berdasarkan metode pengujian yang telah ditentukan. Dari hasil uji 5 (lima) s-box yang baru dibangkitkan kemudian dibandingkan dengan s-box S1 Clefia. Berdasarkan analisis ini, maka didapatkan hasil sbox mana yang memiliki kekuatan minimal sama dengan S1 Clefia.

III. HASIL DAN PEMBAHASAN

A. Hasil Pembangkitan s-box

Pembangkitan s-box berdasarkan metode yang telah disebutkan pada Bab II, menghasilkan 5 buah sbox sebagai berikut :

63	72	C5	98	FD	BD	F4	C4	90	94	1F	37	8C	51	59	DA
DF	36	C6	25	29	47	4	D5	73	B7	1D	91	7E	99	1B	F0
AA	C9	2	CA	D4	23	42	0B	F3	5	2A	87	D3	DE	3B	5E
AD	AE	66	EF	C7	D8	F5	BA	A6	43	8	D0	BF	15	5B	EB
7A	9C	7C	E6	C1	CE	4F	E9	78	5C	F9	E5	D9	70	9D	3
54	E2	89	BE	4E	9A	1	76	32	CC	C3	DB	41	F2	13	92
86	7B	21	B2	BC	F8	34	67	A7	45	79	B3	E0	6D	8B	8E
35	97	8F	B6	7	75	D1	93	71	E8	B4	95	6C	65	DD	10
0D	3E	3C	2E	0A	6E	96	39	2F	A4	85	4A	50	1E	60	A5
48	6F	4D	0E	81	A8	55	9E	68	DC	9B	4B	24	F6	1A	8A
6A	16	52	69	28	B5	4C	19	2D	30	56	2C	14	26	1C	84
6B	CB	AC	0F	82	33	ED	FB	0C	5D	7D	49	62	3A	F7	CF
C8	9	3F	5F	9F	46	74	88	A1	B1	EC	D6	61	38	E4	A3
D7	B0	A9	A2	FE	6	C2	57	7F	2B	3D	AF	58	FF	F1	EA
77	64	83	53	8D	B8	D2	5A	EE	C0	BB	20	31	40	E3	B9
44	E1	FC	AB	A0	18	E7	27	17	0	80	11	CD	22	12	FA

Gambar 2. Sbox 1

63	50	98	A5	F4	85	BD	A4	8C	0D	DA	2E	1F	96	94	6E
73	81	91	9E	1B	4D	99	6F	29	68	D5	4B	C6	1A	36	F6
AD	62	EF	CF	F5	7D	D8	5D	BF	6B	EB	0F	8	ED	43	33
F3	28	87	19	3B	52	DE	16	D4	2D	0B	2C	2	1C	C9	26
86	31	B2	B9	34	BB	F8	C0	E0	77	8E	53	79	D2	45	B8
71	A0	95	27	DD	FC	65	E1	7	17	93	11	8F	12	97	22
54	58	BE	EA	1	3D	9A	2B	41	D7	92	A2	C3	C2	CC	6
78	9F	E5	88	9D	3F	70	9	C1	A1	E9	D6	7C	E4	9C	38
C8	D9	5F	3	74	F9	46	5C	61	7A	A3	E6	EC	4F	B1	CE
7F	4E	AF	76	F1	89	FF	E2	FE	32	57	DB	A9	13	B0	F2
44	6C	AB	10	E7	B4	18	E8	CD	35	FA	B6	80	D1	0	75
EE	BC	20	67	E3	21	40	7B	8D	A7	5A	B3	83	8B	64	6D
6A	D3	69	5E	4C	2A	B5	5	14	AA	84	CA	56	42	30	23
0C	C7	49	BA	F7	66	3A	AE	82	A6	FB	D0	AC	5B	CB	15
48	7E	0E	F0	55	1D	A8	B7	24	DF	8A	25	9B	4	DC	47
2F	FD	4A	C4	60	C5	1E	72	0A	90	39	37	3C	59	3E	51

Gambar 3. Sbox 2

63	98	F4	BD	8C	DA	1F	94	73	91	1B	99	29	D5	C6	36
AD	EF	F5	D8	BF	EB	8	43	F3	87	3B	DE	D4	B	2	C9
86	B2	34	F8	E0	8E	79	45	71	95	DD	65	7	93	8F	97
54	BE	1	9A	41	92	C3	CC	78	E5	9D	70	C1	E9	7C	9C
C8	5F	74	46	61	A3	EC	B1	7F	AF	F1	FF	FE	57	A9	B0
44	AB	E7	18	CD	FA	80	0	EE	20	E3	40	8D	5A	83	64
6A	69	4C	B5	14	84	56	30	C	49	F7	3A	82	FB	AC	CB
48	E	55	A8	24	8A	9B	DC	2F	4A	60	1E	A	39	3C	3E
4B	68	F6	1A	9E	81	6F	4D	2E	D	6E	96	A5	50	A4	85
2C	2D	26	1C	19	28	16	52	F	6B	33	ED	CF	62	5D	7D
11	17	22	12	27	A0	E1	FC	53	77	B8	D2	B9	31	C0	BB

D6	A1	38	E4	88	9F	9	3F	A2	D7	6	C2	EA	58	2B	3D
DB	32	F2	13	76	4E	E2	89	E6	7A	CE	4F	3	D9	5C	F9
B3	A7	6D	8B	67	BC	7B	21	B6	35	75	D1	10	6C	E8	B4
D0	A6	15	5B	BA	C7	AE	66	CA	AA	23	42	5E	D3	5	2A
37	90	51	59	C4	FD	72	C5	25	DF	47	4	F0	7E	B7	1D

Gambar 4. Sbox 3

62	1E	7B	46	79	28	5E	10	91	DA	52	3B	95	D6	1C	9
F9	C4	0	DF	E1	FF	CE	F7	EE	1B	B6	AD	61	A0	ED	B5
76	14	24	41	A1	8B	B2	FD	2A	70	9F	E4	EA	BE	11	9C
4E	72	B3	3A	9E	A5	9D	85	3D	94	55	66	8D	60	C2	58
36	86	E6	49	4F	AA	69	7E	9B	F	81	2F	21	BB	E	39
31	5F	6C	88	12	7D	4B	8A	D3	E0	4A	C8	51	A4	80	AE
F8	AC	23	2E	20	EF	3F	77	A7	3	C3	99	25	5B	6F	45
5D	71	FB	1F	6	26	2B	FC	CB	4D	29	EB	BF	1D	96	AB
E2	13	8F	1A	5C	56	C6	DC	D5	D1	A9	F3	F6	B	7	78
6E	4	53	57	CD	27	9A	40	84	BD	67	B7	AF	73	38	A6
D4	C7	C5	B4	65	A	92	BA	47	F1	F0	15	37	7C	68	C0
2	CC	BC	FA	DD	42	43	8C	32	D	A2	7F	35	C1	89	B8
2D	63	E7	D2	98	5	DB	4C	1	B9	33	93	C9	B1	97	90
CF	87	5A	30	D8	E9	6D	C	54	8E	D7	17	82	22	2C	CA
75	6B	48	74	16	44	83	64	D0	B0	EC	3C	FE	3E	E3	F2
59	6A	18	34	A8	50	DE	A3	F5	8	19	D9	7A	E8	F4	E5

Gambar 5. Sbox 4

EA	7C	9	D6	4A	A2	6	2A	F3	50	2B	F	3E	AE	B6	70
84	5F	AA	E4	39	17	C0	2F	D1	F7	AB	75	A9	E7	E5	6A
7B	59	76	D8	DE	26	72	56	3B	B4	1D	FD	9F	82	28	4D
F4	5	CF	5E	29	FF	85	57	A4	91	C8	E	25	5D	20	3F
D	3	8	D5	4B	CC	93	44	95	2C	3A	67	6B	F0	33	74
27	C7	63	4	AD	3C	BC	11	92	CA	64	2D	8E	79	7	23
C	47	FA	37	B9	D2	19	F9	BB	90	98	38	71	2	F2	CD
A0	10	86	CE	AF	13	D4	C5	83	40	FB	62	73	51	C4	49
42	1F	9E	9B	22	E2	34	6F	4C	E8	9C	1C	1	12	68	88
54	D9	B8	AC	EF	EB	7F	61	F8	DC	8D	1B	CB	97	2E	D0
48	87	B	DA	77	BD	F5	8F	69	BA	80	BE	4E	89	55	A1
B7	14	16	C2	4F	66	45	35	C3	65	60	8A	3D	E9	0	8C
5A	C1	7D	43	C6	18	E3	B5	24	5B	9D	F6	53	8B	E6	A3
78	C9	21	9A	E0	A5	1E	94	58	52	E1	A7	46	D3	1A	B0
7E	A	FE	81	D7	A6	B1	F1	DB	36	5C	DF	30	FC	BF	15
EC	6C	7A	96	6D	A8	B2	41	31	32	ED	6E	EE	DD	B3	99

Gambar 6. Sbox 5

B. Hasil Pengujian s-box baru

Berdasarkan metode yang telah ditentukan, pengujian terhadap sbox yang telah dibangkitkan, menghasilkan hasil uji sebagai berikut :

Tabel 1. Hasil Pengujian sbox baru

Nama Pengujian	Sbox 1	Sbox 2	Sbox 3	Sbox 4	Sbox 5
LAT	16	16	16	34	36
XOR Table	4	4	4	10	12
Nonlinearity	112	112	112	94	92
SAC	0,0625	0,0625	0,0625	0,1093	0,125
BIC	0,1285	0,1341	0,1341	0,2649	0,2834

S1 Clefia berdasarkan pengujian tersebut memiliki nilai *LAT* maksimal sebesar 16, nilai *differential uniformity* (*XOR Table*) sebesar 4 dan nilai *nonlinearity* 112. Selain itu S1 Clefia memiliki hasil uji *Max Error* SAC sebesar 0,0625 dan nilai BIC sebesar 0,131696.

C. Analisis Hasil Uji

Analisis hasil uji yang telah dilakukan adalah sebagai berikut :

1. LAT

Pada pengujian *LAT* diketahui bahwa sbox 1, sbox 2 dan sbox 3 memiliki nilai LAT yang sama dengan S1 Clefia yaitu 16. Dari hasil ini diperoleh bahwa probabilitas bias terbaik untuk melakukan *linear cryptanalysis* yaitu 1/16 ≈ 0,062. Sedangkan untuk sbox 4 memiliki probabilitas sebesar 34/256 ≈ 0,1328 dan sbox 5 sebesar 36/256 ≈ 0,1406. Untuk lebih memahami tingkat kekuatan berdasarkan nilai tersebut, diberikan penjelasan berikut :

Jika diasumsikan suatu algoritma memiliki kompleksitas sbox aktif sebesar 50. Penggunaan sbox hasil pembangkitan menyebabkan algoritma tersebut memiliki tingkat kekuatan berdasarkan serangan *linear cryptanalysis* seperti pada Tabel 2.

Tabel 2. Tingkat Kekuatan Sbox pada Algoritma (*Linear Cryptanalysis*)

Sbox	Prob. bias box	Kompleksitas Serangan	Kekuatan Algoritma
S1 Clefia	0,062	$6{,}22\ x\ 10^{61}$	200
Sbox 1	0,062	$6{,}22\ x\ 10^{61}$	200
Sbox 2	0,062	$6{,}22\ x\ 10^{61}$	200
Sbox 3	0,062	$6{,}22\ x\ 10^{61}$	200
Sbox 4	0,1328	$1{,}45\ x\ 10^{44}$	146
Sbox 5	0,1406	$2{,}53\ x\ 10^{43}$	141

2. *XOR Table*

Pada pengujian *XOR Table* diketahui bahwa sbox 1, sbox 2 dan sbox 3 memiliki nilai *XOR Table* yang sama dengan S1 Clefia yaitu 4. Dari hasil ini diperoleh bahwa probabilitas terbaik untuk melakukan *differential cryptanalysis* yaitu 4/256 ≈ 0,0156. Sedangkan untuk sbox 4 memiliki probabilitas sebesar 34/256 ≈ 0,039 dan sbox 5 sebesar 36/256 ≈ 0,0468. Untuk lebih memahami tingkat kekuatan berdasarkan nilai tersebut, diberikan penjelasan berikut :

Jika diasumsikan suatu algoritma memiliki kompleksitas sbox aktif sebesar 50.. Penggunaan sbox hasil pembangkitan menyebabkan algoritma tersebut memiliki tingkat kekuatan berdasarkan serangan *differential cryptanalysis* seperti pada Tabel 3.

Tabel 3. Tingkat Kekuatan Sbox pada Algoritma (*differential Cryptanalysis*)

Sbox	Prob. bias box	Kompleksitas Serangan	Kekuatan Algoritma
S1 Clefia	0,0156	$4{,}90\ x\ 10^{91}$	300
Sbox 1	0,0156	$4{,}90\ x\ 10^{91}$	300
Sbox 2	0,0156	$4{,}90\ x\ 10^{91}$	300
Sbox 3	0,0156	$4{,}90\ x\ 10^{91}$	300
Sbox 4	0,0390	$3{,}87\ x\ 10^{71}$	233
Sbox 5	0,0468	$3{,}52\ x\ 10^{67}$	220

3. *Nonlinearity*

Berdasarkan hasil pengujian *nonlinearity* pada Tabel 1, sbox 4 dan sbox 5 memiliki nilai nonlinearity yang lebih rendah dari S1 Clefia. Nilai *nonlinearity* kedua sbox tersebut jauh dari kriteria *perfect nonlinearity* dimana untuk ukuran 8x8 sebesar 120.

4. *SAC*

Pada pengujian ini, nilai *Max Error* SAC sbox 1, sbox 2 dan sbox 3 sebesar < 0,1. Sedangkan sbox 4 dan sbox 5 memiliki nilai *Max Error* SAC > 0,1. Dengan demikian sbox 4 dan sbox 5 tidak memiliki difusi yang baik berdasarkan kriteria SAC

5. *BIC*

Pada pengujian ini, nilai korelasi maksimal sbox 1, sbox 2 dan sbox 3 sebesar < 0,2. Sedangkan sbox 4 dan sbox 5 > 0,2. Dengan demikian sbox 4 dan sbox 5 tidak memiliki difusi yang baik berdasarkan kriteria BIC

Berdasarkan analisa yang telah dilakukan, disimpulkan bahwa sbox 1, sbox 2 dan sbox 3 memiliki tingkat kekuatan yang menyerupai S1 Clefia. Sedangkan sbox 4 dan sbox 5 memiliki tingkat kekuatan lebih buruk dibanding S1 Clefia.

IV. KESIMPULAN

Berdasarkan penelitian, pengujian dan analisis pada paper ini, diambil kesimpulan sebagai berikut :

1. Sbox yang dibangkitkan dengan menambahkan fungsi linear terhadap S1 Clefia pada penelitian ini (sbox 1, sbox 2 dan sbox 3) memiliki tingkat kekuatan yang menyerupai S1 Clefia.
2. Sbox yang dibangkitkan dengan menambahkan fungsi nonlinear, maupun kombinasi fungsi linear dan nonlinear terhadap S1 Clefia pada penelitian ini (sbox 4 dan sbox 5) memiliki tingkat kekuatan yang lebih buruk dari S1 Clefia.
3. Fungsi linear maupun kombinasinya dapat dijadikan alternatif untuk membangkitkan sbox baru dari sbox yang sudah ada tanpa mengurangi kekuatannya.

DAFTAR PUSTAKA

[1] Dundar, Baha Guclu. *Cryptographic Properties of Some Highly Nonlinear Balanced Boolean Functions*. Department of Cryptography-Ocak: Turkey. 2006.

[2] Budaghyan, Lilya. *The Equivalence Of Almost Bent and Almost Perfect Nonlinear Functions and Their Generalizations*: Dissertation. 2005.

[3] E. Biham & A. Shamir. "Differential Cryptanalysis of DES-Like Cryptosystems," Journal of Cryptology, volume:4 pp. 3-72: Norway. 1991.

[4] Howard M. Heys. *A Tutorial on Linear and Differential Cryptanalysis.* Memory University of Newfoundland, Canada

[5] M. Matsui. Linear Cryptanalysis Method for DES cipher, Lectures Notes in Computer Science no. 765, Springer Verlag, pp. 386-397: Japan. 1994.

[6] Sony Corporation. The 128-bit Blockcipher CLEFIA : Japan. 2007.

[7] Webster A. F., Tavares S. E. On The Design Of S-BOXES. Queens's University:Canada